

**Claims**

1. A method in a communication system wherein a serving controller is configured to support a first security mechanism and at least one other security mechanism, the method comprising:
  - 5 sending a request for registration from a user equipment to a serving controller;
  - determining, based on the request, in a second controller that the user equipment supports a second security mechanism other than a first security mechanism;
  - 10 sending from the second controller to the serving controller an indication that the second security mechanism than the first security mechanism is used by the user equipment; and
  - 15 sending a challenge in accordance with the second security mechanism from the serving controller to the user equipment.
- 20 2. A method as claimed in claim 1, further comprising:
  - including a response to the challenge in a message from the user equipment to the serving controller.
3. A method as claimed in claim 2, further comprising:
  - 25 using the response for authentication of the message at the serving controller.
4. A method as claimed in claim 1, further comprising:
  - 30 providing the second controller comprising a network entity providing proxy call state control functions between the user equipment and the serving controller.

5. A method as claimed in claim 1, wherein the step of sending the request for registration from the user equipment to the serving controller comprises
- 5 sending a challenge from the serving controller to the user equipment, sending a response to the challenge from the user equipment, and
- registering the user equipment to the serving controller only if a satisfactory response is received from the user equipment,
- 10 and sending a further challenge to the user equipment after the registration step is completed.
6. A method as claimed in claim 1, further comprising:
- 15 obtaining data for sending the challenge from a user information database.
7. A method as claimed in claim 1, wherein the step of sending the challenge comprises sending the challenge comprising an authentication vector.
- 20
8. A method as claimed in claim 1, further comprising:
- providing the first security mechanism comprising a security mechanism in accordance with a Secure Internet Protocol.
- 25
9. A method as claimed in claim 1, wherein the further comprising:
- providing the second security mechanism comprising a security mechanism in accordance with a Hypertext Transfer
- 30 Digest protocol.
10. A method as claimed in claim 1, further comprising:

sending of at least the challenge or a response in a message in accordance with a Session Initiation Protocol.

11. A method as claimed in claim 1, further comprising:

5        registering the user equipment with a serving controller of an Internet Multimedia Subsystem.

12. A method as claimed in claim 2, further comprising:

10        including in a security-client header of the request for registration a list of security mechanisms supported by the user equipment;

         concluding at the second controller based on the list that the user equipment supports the second security mechanism instead of the first security mechanism;

15        removing the security-client header from the request and including into an authorization header of the request an indication that the second security mechanism is to be used; and

         forwarding the request to the serving controller.

20

13. A method as claimed in claim 1, wherein the step of sending the challenge comprises sending the challenge to the user equipment in an authentication information header of a message.

25

14. A method as claimed in claim 3, further comprising:

         providing the message comprising a request for a service provided by an application server.

30

15. A communication system comprising:

a serving controller configured to accept registrations of user equipments and to support at least two different security mechanisms; and

means for providing the serving controller with  
5 information regarding a security mechanism supported by a user equipment that has requested for registration to the serving controller, wherein the serving controller is configured to send a challenge in accordance with a determined security mechanisms to the user equipment and to  
10 authenticate a message from the user equipment based on a response to the challenge included in the message.

16. A communication system as claimed in claim 15, wherein the means for providing information regarding a supported  
15 security mechanism are provided in a second controller.

17. A communication system as claimed in claim 16, wherein the second controller comprises a network entity providing proxy call state control functions between the user equipment  
20 and the serving controller.

18. A communication system as claimed in claim 15, further comprising:

a user information database configured to store data  
25 associated with challenges.

19. A communication system as claimed in claim 15, wherein the serving controller is configured to support a security mechanism in accordance with a Secure Internet Protocol.  
30

20. A communication system as claimed in claim 15, wherein the serving controller is configured to support a security

mechanism in accordance with a Hypertext Transfer Digest protocol.

21. A communication system as claimed in claim 15, the  
5 communication system comprising an Internet Multimedia Subsystem.

22. A communication system as claimed in claim 15, further comprising:  
10 a connection to an application server, wherein a message subjected to authentication by the servicing controller based on the response to the challenge comprises a request for a service provided by the application server.

15 23. A communication system as claimed in claim 15, wherein the message subjected to authentication by the servicing controller based on the response to the challenge comprises a request for registration to the serving controller.

20 24. A proxy controller for a communication system, the proxy controller being configured to forward registrations of user equipments to a serving controller, to determine a security mechanism supported by a user equipment that has requested for registration to the serving controller, and to signal  
25 information to the serving controller regarding the security mechanism supported by the user equipment.

25. A communication system comprising:  
first sending means for sending a request for  
30 registration from a user equipment to a serving controller;  
determining means for determining, based on the request, in a second controller that the user equipment supports a

second security mechanism other than a first security mechanism;

second sending means for sending from the second controller to the serving controller an indication that the  
5 second security mechanism other than the first security mechanism is used by the user equipment; and

third sending means for sending a challenge in accordance with the second security mechanism from the serving controller to the user equipment.